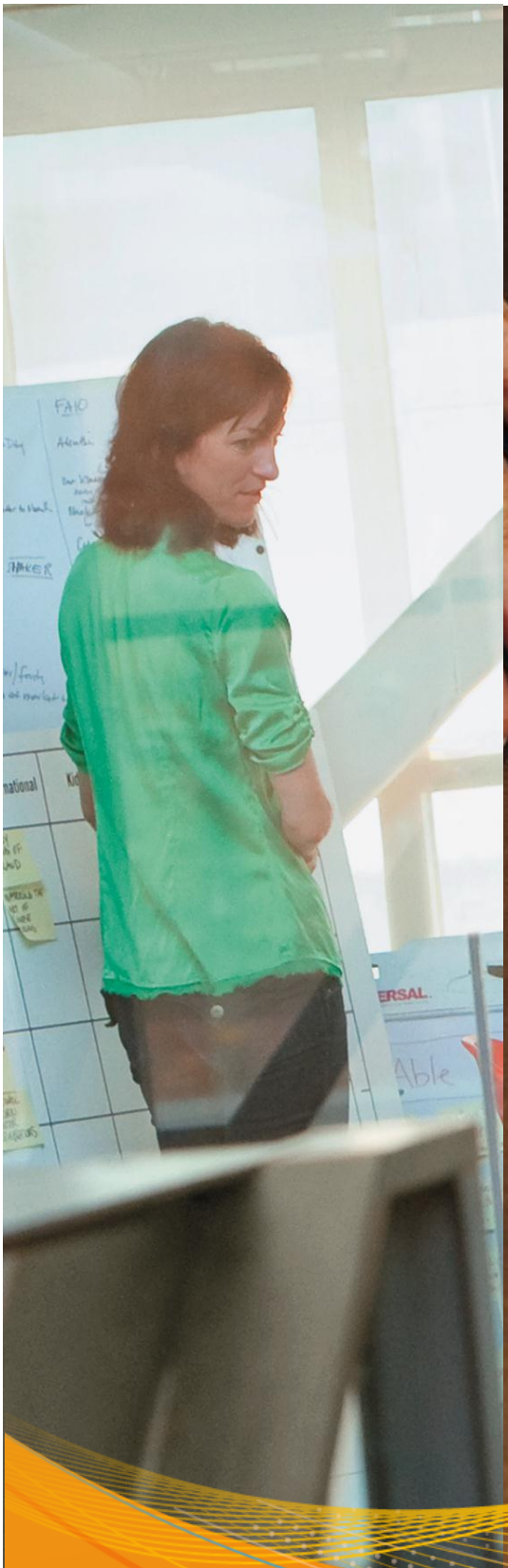

Security in Office 365

Whitepaper

Published: June 2011

Microsoft® Office 365

Microsoft

Table of Contents

Introduction

This paper provides an overview of the security practices and technology that support enterprise-grade security in Microsoft Office 365 for businesses of all sizes. For a comprehensive and detailed treatment of security in Office 365, download the Office 365 Security Service Description, available at http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6c6ecc6c-64f5-490a-bca3-8835c9a4a2ea.

Microsoft® Office 365 delivers the power of cloud productivity to businesses of all sizes, helping to save time and money and free up valued resources. Office 365 combines the familiar Office desktop suite with cloud-based versions of our next-generation communications and collaboration services: Microsoft Exchange Online, Microsoft SharePoint® Online and Microsoft Lync™ Online.

When allowing an external service provider to store and manage their data, companies and other organizations must consider security, data protection, privacy, and data ownership. Microsoft takes these concerns seriously and has applied its years of cloud and on-premises experience with security and privacy to the Office 365 services. Microsoft Online Services can help you get the benefits of cloud computing with the enterprise-grade security you require, whatever the size of your organization. Microsoft takes a comprehensive approach to protecting your data at both the physical layer (exemplified by our $2 billion investment in state-of-the-art data centers) and the logical layer (for example, with security-aware engineering practices for services and software).

Office 365 provides secure access across platforms and devices, as well as premium anti-spam and antivirus technologies that are automatically updated to protect against the latest threats. The security features and services associated with Office 365 are built in, reducing the time and cost associated with securing your IT systems. At the same time, Office 365 enables you to easily control permissions, policies, and features through online administration and management consoles so you can configure Office 365 to meet your specific security needs.

Challenges

With more workers on the go, your business information is likely accessed by more people and from more places and platforms than ever before. However, this increased access also increases the attack surface of IT. And, those attacks become more and more sophisticated and malicious. Today, cybercrime is perpetrated by highly organized, financially motivated professional criminals. A comprehensive approach to security is required to protect your systems and data in this environment. Microsoft's end-to-end approach to security includes engineering more secure services and software, effectively monitoring and responding to threats, and researching emerging threats to protect against them before they become problems. With continuing rapid growth in the sheer quantity of data generated by ordinary business operations, data backup and recovery have become major cost centers for IT departments today. Organizations need scalable, affordable solutions for ensuring their data is available 24/7.

Given these many challenges, many organizations discover that Office 365 can provide a higher standard of security at lower cost than they are capable of maintaining with on-premises productivity servers. Office 365 customers are freed from the costly burden of deploying and managing antivirus, anti-spam, backup, and disaster recovery solutions in-house. Office 365 provides built-in scalability and disaster recovery to accommodate growing volumes of business-critical data—all for a fixed, predictable cost. Distinct from other cloud productivity vendors' offerings, Office 365 provides the flexibility to temporarily or permanently maintain a hybrid environment so you can move to the cloud gradually or maintain some users on-premises indefinitely.

A secure foundation

Microsoft has been providing online services for many years. Microsoft Global Foundation Services (GFS), the group responsible for hosting Office 365 and all of Microsoft's online services, started in 1994 with the introduction of MSN and has grown to include some of the world's most well-known Internet properties. The online services infrastructure layer (GFS) is regularly audited by respected third party organizations. Through our comprehensive approach to security and privacy, Microsoft Global Foundation Services has obtained ISO 27001 and EU Safe Harbor certification and successfully completed SAS 70 Type II audit. Office 365 is based on proven technology, representing the latest generation of what was formerly known as Business Productivity Online Services (BPOS) with hundreds of thousands of satisfied customers. With Office 365, you benefit from this deep experience in the cloud.

Microsoft recognizes that security is an ongoing process, not a steady state—it must be constantly maintained, enhanced, and verified by experienced and trained personnel; supported by up-to-date software and hardware technologies; and refined through robust processes for designing, building, operating, and supporting our services.

Office 365 data is stored in Microsoft's own network of highly available data centers, strategically located around the world. These facilities are built from the ground up to protect services and data from harm, whether natural disaster or unauthorized access. Physical security best practices are maintained, including state-of-the-art hardware, 24-hour secured access, redundant power supplies, multiple fiber trunks, and other features. Because of system redundancy, updates can generally be deployed to the system without any downtime for your users. The system is protected at the logical layer by robust data isolation, continuous monitoring, and a wide array of other recognized practices and technologies. All of the physical and logical security tasks are taken care of in the data center, which can drastically reduce the amount of time you spend keeping your data and systems safe.

Since 2002, Microsoft has promoted security best practices internally and in the industry through the Trustworthy Computing initiative. An important part of Trustworthy Computing is engineering software that is more secure from the beginning. To this end, the products and services that make up Office 365—Microsoft Exchange Online, Microsoft SharePoint® Online, Microsoft Lync® Online, and Microsoft Office Professional Plus—were designed and built according to the rigorous security practices encoded in the

Microsoft Security Development Lifecycle (SDL). The SDL is constantly updated and freely shared within the software industry to help drive better security practices across vendors and platforms.

You need to ensure that business data is continuously available to your users. Because of Microsoft experience in hosting services as well as the close relationship between Office 365 and the Microsoft product and support teams, Office 365 can meet the high continuity standards customers demand. Service continuity protocols and technologies enable Office 365 to recover quickly from unexpected outages.

Privacy and data ownership

Microsoft provides a coherent, robust, and transparent privacy policy emphasizing that you maintain ownership of your data. The Trust Center (available at the time of General Availability) tells you exactly how we handle and use data gathered in your interactions with Microsoft Online Services. If you decide to stop using Office 365, by default we provide 90 days of reduced functionality service, allowing you to export your data. Microsoft also provides multiple notices prior to deletion of customer data.

Separation of customer data

Office 365 is a multi-tenant service, meaning that data is distributed among hardware resources. Therefore, your data may be stored on the same hardware as that of other customers. This is one reason that Office 365 can provide the cost and scalability benefits that it does. Microsoft goes to great lengths to ensure that the multi-tenant architecture of Office 365 supports enterprise privacy and security standards. Data storage and processing is logically segregated between customers through specialized Active Directory technology engineered specifically for the purpose. For organizations that want additional data isolation, a version of Office 365 is available that stores your data on dedicated hardware.

Built-in Security

Unlike an on-premises installation that lives behind a corporate firewall and may be accessed over a virtual private network (VPN), Office 365 is designed specifically for secure access over the Internet. There are two options for user identification: Microsoft Online IDs and Federated IDs. In the first case, users create Microsoft Online Services accounts for use with Office 365. Users sign in to all their Office 365 services using a single login and password. The single sign-on application helps users easily create and use strong passwords that keep their services safe.

You can also choose federated identification, which uses on-premises Active Directory Federation Services (a service of Microsoft Windows Server 2008) to authenticate users on Office 365 using their corporate ID and password. In this scenario, identities are administered only on-premises. This also enables

organizations to use two-factor authentication (such as smart cards or biometrics in addition to passwords) for maximum security.

Regardless of how users sign in, connections established over the Internet to the Office 365 service are encrypted using industry-standard, 128-bit Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption. Office 365 supports additional security measures to protect sensitive information such as Secure/Multipurpose Internet Mail Extensions (S/MIME) for public key encryption and digital signatures as well as Information Rights Management protection for restricting who can access and perform specific actions on documents, email, and even voicemail messages.

With Office 365, you have complete access to your environment including user mailboxes, SharePoint Web sites and document stores. You maintain control over security policies and user accounts. This degree of control enables you to enforce your company's privacy and security policies effectively. Policies and users can be managed using a Web-based management console or Remote PowerShell for automation of routine tasks.

Forefront Online Protection for Exchange

To protect incoming, outgoing, and internal email and shared files against viruses and spam, Office 365 includes Microsoft Forefront® Online Protection for Exchange. This multi-layered antivirus/anti-spam solution uses multiple scanning engines for highly accurate identification and mitigation of threats while minimizing "false positives" that can lead to improperly blocked email. Forefront technologies included with Office 365 are constantly updated with the latest threat signatures, helping to protect you from new and emerging threats without any additional work on your part.

Flexibility to meet advanced security needs

Some organizations may face industry, regulatory or internal security requirements that go beyond what is offered in a distributed multitenant environment. For example, they may have restrictions on which countries data can be stored in, or need to keep all data within a certain country. Microsoft has designed the Office 365 to provide maximum flexibility for organizations to choose how they deploy. You can deploy Microsoft Exchange Server, Microsoft SharePoint® Server, and Microsoft Lync® Server on-premises today and easily move to the cloud later. You can choose to keep some users on-premises and have others in the cloud using coexistence, giving both sets of users the ability to see each other's free/busy information, share calendars, and communicate almost as if they were all using the same infrastructure.

Conclusion

Moving productivity services to the cloud requires a serious consideration of security and privacy issues and technologies. Office 365 is designed to deliver the enterprise-grade security you require to move to the cloud with confidence. Our data centers are designed, built, and managed using a defense-in-depth strategy at both the physical and logical layers, and our services are engineered to be secure using the Security Development Lifecycle. Office 365 makes it easy for users and administrators to access and use data and services while following security best practices. We have built our cloud-based productivity services with you in mind, helping you embrace the advantages of the cloud on your terms and at your own pace.

Resources

Office 365: http://office365.microsoft.com

Microsoft Global Foundation Services: http://www.globalfoundationservices.com

Microsoft Data Center Videos: http://www.globalfoundationservices.com/infrastructure/videos.html

Microsoft Trustworthy Computing: http://www.microsoft.com/about/twc/en/us/default.aspx

Security Development Lifecycle: http://www.microsoft.com/security/sdl/default.aspx

Forefront Online Protection for Exchange: http://technet.microsoft.com/en-us/forefront/cc540243